

Remarks

Claims 1-23 remain in the application. Claims 1-3, 6, 14-17 and 20-21 are hereby amended. No new matter is being added.

Substance of Examiner Interview

In a teleconference with the Examiner on November 26, 2007, substantive differences in mirroring of the claimed invention versus the cited references were discussed. In particular, it was discussed how the claimed invention pertained to remote mirroring where a copy of a packet is sent to a separate mirroring destination, while the original packet is still forwarded to its original destination. In contrast, the cited art does not pertain to mirroring and so does not send a separate copy to a separate mirroring destination while still forwarding the packet to the original destination.

Claim Rejections

Claims 1-23 were rejected under 35 USC 102 and/or 103(a) as being anticipated by Amara et al (USP 6,839,338) or as being unpatentable over Amara et al in combination with one or more other references (including Liu et al, Kojima et al, Classon et al, and Engwer). Applicants respectfully traverse these rejections in relation to the claims as hereby amended.

Amended claim 1 now recites as follows.

1. A method for secure remote mirroring of network traffic, the method comprising:
 - receiving a data packet to be remotely mirrored by an entry device pre-configured with a mirroring destination address to which to mirror the data packet;
 - forwarding the data packet in unencrypted form towards an original destination address indicated in the data packet;**
 - encrypting a copy of the data packet to form an encrypted packet;
 - incrementing an identifier for indicating a position of the encrypted packet within an order of packets received by the entry device for remote mirroring;

generating and adding a header to encapsulate the encrypted data packet, wherein
the header includes the mirroring destination address and said identifier;
and
**forwarding the encapsulated encrypted packet to an exit device associated
with the mirroring destination address.**

(Emphasis added.)

As seen above, amended claim 1 now recites further limitations which are specific to **mirroring**. The ZDNet Dictionary, for example, defines mirroring as “Duplicating data onto another computer at another location. Mirroring is performed for backup purposes or to be in closer proximity to the user.” (See <http://dictionary.zdnet.com/definition/Mirroring.html>.)

As the present application pertains to mirroring, claim 1 now recites both (1) “forwarding the data packet in unencrypted form towards an original destination address indicated in the data packet” and (2) “forwarding the encapsulated encrypted packet to an exit device associated with the mirroring destination address.” Regarding (1), the present application states, for example, “In one particular embodiment, the entry device may comprise an Ethernet type switch as depicted in FIG. 1. ... When packets are destined for IP addresses ... those packets may be forwarded to their destination” (Page 4, lines 25-32.) Regarding (2), the present application states, for example, “Preliminarily, the entry device 102 may be pre-configured 202 with a mirror source and a mirror destination and with an encryption key. ... the mirror destination is the destination to which the mirror packets are to be securely sent.” (Page 6, lines 21-24.)

In other words, in the claimed invention, while the original packet is sent to its original destination, an encrypted copy of the packet is sent separately to the mirroring destination.

Amara et al does not pertain to mirroring of traffic between an entry device and an exit device. Instead, Amara et al relates to using IP security so that a mobile node may communicate securely to its home network.

Because Amara et al does not pertain to mirroring, Amara et al does not perform both “forwarding the data packet in unencrypted form towards an original destination address indicated in the data packet” and “forwarding the encapsulated encrypted packet to an exit device associated with the mirroring destination address.”

In fact, Amara et al discloses a technique which in some respect teaches against the claimed invention. The technique of Amara et al is used to provide Internet Protocol security. One problem discussed in Amara et al is that “Other devices may intercept the IP packet and read its data portion.” The IP security discussed in Amara et al prevents such interception and reading. While the claimed invention encrypts the **mirrored** packet that is sent to the mirroring destination, the claimed invention does not encrypt the **original** packet that is forwarded to its original destination and so goes against this teaching of Amara et al.

Similarly, the other cited references also do not pertain to mirroring. Hence, they do not teach both “forwarding the data packet in unencrypted form towards an original destination address indicated in the data packet” and “forwarding the encapsulated encrypted packet to an exit device associated with the mirroring destination address.”

Therefore, applicants respectfully submit that claim 1, as hereby amended, now overcomes these rejections for at least the above-discussed reasons.

Claims 2-13 depend from claim 1. Hence, applicants respectfully submit that these claims now also overcome these rejections for at least the same reasons discussed above in relation to claim 1.

Independent claims 14, 17, 20, and 21 are amended with similar limitations as claim 1. For example, claim 17 specifies that “the pre-configured destination” to which “encrypted copies of the detected packets” are forwarded for purposes of mirroring “is distinct from original destinations indicated in the detected packets.” Hence, applicants respectfully submit that claims 14, 17, 20, and 21 now overcome these rejections for at least the same reasons discussed above.

Claims 15-16 depend from claim 14, claims 18-19 depend from claim 17, and claims 22-23 depend from claim 21. Hence, applicants respectfully submit that these dependent claims now also overcome these rejections for at least the same reasons discussed above.

Further regarding claim 10, applicants further submit that the citations to the abstract and column 8 lines 66 – column 9, line 15 of Amara et al do not disclose the recited limitation of “configuring the entry device **in a best effort mirroring mode to reduce head-of-line blocking.**” (Emphasis added.) Applicants respectfully submit that no such best effort mirroring mode to reduce head-of-line blocking is taught or suggested by the specified citations.

For convenience of reference, the abstract and column 8 lines 66 – column 9, line 15 of Amara et al are reproduced below. As seen below, no best effort mirroring mode to reduce head-of-line blocking is taught or suggested by the specified citation.

Abstract

A mobile node may roam away from its home network to a foreign network. The mobile node may communicate using the Mobile Internet Protocol, and it may use Internet Protocol security to communicate with its home network. A foreign agent on the foreign network and a home agent on the home network may dynamically link a policy to be used for a Internet Protocol security session between the foreign agent and the home agent. The foreign agent and the home agent may dynamically create a filter to be used for the Internet Protocol Security session.

Column 8 lines 66 – column 9, line 15

In the tunnel mode generally the entire IP packet is encrypted, and it is sent along a virtual tunnel to the destination device. A virtual tunnel can be formed using a router or other network device that acts as an IPsec proxy for the source device and the destination device. The source device sends an IP packet to a source device endpoint. The source device endpoint encrypts the IP packet, and

it places the encrypted packet into a new IP packet. The new IP packet is then sent through the network to a destination device endpoint. The destination device endpoint decrypts the original IP packet, and it forwards that packet to the destination device. Using this mode, an attacker can only determine the endpoints of the tunnel. The attacker cannot determine the actual source and destination addresses of the tunneled packet, and, therefore, the attacker cannot accurately determine how many packets are being sent between two devices.

Further regarding claim 12, applicants further submit that combining **truncation** to satisfy buffer requirements from Classon would be problematic in combination with the system of Amara et al. This is because truncating packets per Classon would result in **missing data** in the communications of Amara et al (where packets are communicated from a mobile node to a home network). In contrast, truncation is acceptable in accordance with the present application because copies of the packets are being transmitted for monitoring purposes. Therefore, applicants respectfully submit that claim 12 overcomes its rejection.

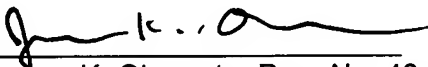
Conclusion

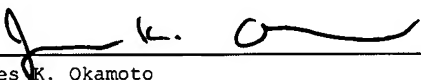
For the above-discussed reasons, applicant believes that the pending claims, as they are hereby amended, now overcome the claim rejections. Favorable action is respectfully requested.

If for any reason an insufficient fee has been paid, the Commissioner is hereby authorized to charge the insufficiency to Deposit Account No. 08-2025 (Hewlett Packard).

Respectfully Submitted,

Dated: December 21, 2007


James K. Okamoto, Reg. No. 40,110
Okamoto & Benedicto LLP
P.O.Box 641330
San Jose, CA 95164-1330
Tel: (408) 436-2111
Fax: (408) 436-2114

CERTIFICATE OF MAILING			
I hereby certify that this correspondence, including the enclosures identified herein, is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below. If the Express Mail Mailing Number is filled in below, then this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 CFR 1.10.			
Signature:			
Typed or Printed Name:	James K. Okamoto	Dated:	12/21/2007
Express Mail Mailing Number (optional):			